IN THE UNITED STATES DISTRICT COURT FOR THE
EASTERN DISTRICT OF VIRGINIA

Alexandria Division

IN THE MATTER OF THE SEARCH OF: APPLE IPAD WITH SERIAL NUMBER GG7FK29GQ16X AND PREDATOR HELIOS NEO 16 LAPTOP WITH SERIAL NUMBER NHQMAAA0013140C5E77600 LOCATED AT FBI WASHINGTON FIELD OFFICE, NORTHERN VIRGINIA RESIDENT AGENCY, MANASSAS, VIRGINIA	Case No. 1:24-SW-392

AFFIDAVIT IN SUPPORT OF AN APPLICATION UNDER RULE 41 FOR A WARRANT TO SEARCH AND SEIZE

I, Jordan Jenkins, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant authorizing the examination of property associated with ROBERT WESLEY ROBB (hereinafter "ROBB"), specifically one Apple iPad with serial number GG7FK29GQ16X and one Predator Helios Neo 16 laptop with serial number NHQMAAA0013140C5E77600 (hereinafter referred to as the **SUBJECT DEVICES)**, which are currently in law enforcement possession and located at the FBI's Washington Field Office, Northern Virginia Resident Agency, in Manassas, Virginia, which is within the Eastern District of Virginia, and the extraction from that property of electronically stored information described in Attachment B.

2. I have been a Special Agent with the Federal Bureau of Investigation (FBI), and I have been so employed for since 2021. I am currently assigned to the FBI's Washington Field Office's securities fraud squad, which has investigative responsibility for complex financial crimes.

I have participated in investigations involving securities fraud, investment fraud, money laundering, and cybercrime. I have training and experience in the enforcement of the laws of the United States, including the preparation and presentation of search warrant affidavits and the execution of search warrants, as well as extensive training in investigating white-collar crimes. I have received the Chainalysis Ethereum Investigations and Certified Anti-Money Laundering certifications, and training in the tracing of funds generated from illicit activity, including cryptocurrencies, through the international banking system and blockchain.

3. In the course of my training and experience, I have had experience with various forms of electronic evidence, such as cell phone data and social media evidence, as it relates to criminal activity. As a federal agent, I am authorized to investigate the violations of laws of the United States, and as a law enforcement officer, I am authorized to execute warrants issued under the authority of the United States.

4. I submit that the following information establishes probable cause to believe that that within the Items To be Searched—as described in Attachment A—there is located evidence, fruits, and instrumentalities of probable violations of 18 U.S.C. §§ 1343 (Wire Fraud), 1956(a)(1)(B)(ii) (Concealment Money Laundering), and 1957 (Unlawful Monetary Transactions) (hereinafter the "Specified Federal Offenses")—as described in Attachment B.

5. The facts in this affidavit come from my personal observations, my training and experience, and information obtained from other law enforcement officers and witnesses. This affidavit is intended to show merely that there is probable cause for the requested warrant and does not set forth all of my knowledge about this matter. Unless specifically indicated, all conversations and statements described in this affidavit are related in substance, and in part only, and are not intended to be a verbatim recitation of such statements. I submit this application for authorization

to search the **SUBJECT DEVICES** for evidence of violations of the Specified Federal Offenses. Based upon the information contained in this application, I have reason to believe that evidence of these violations is located on the **SUBJECT DEVICES**. The applied-for warrant would authorize the forensic examination of the **SUBJECT DEVICES** for the purpose of identifying electronically stored data particularly described in Attachment B.

PROBABLE CAUSE

A. Arrest of ROBB on March 20, 2024

6. On March 15, 2024, a criminal complaint was issued in the Eastern District of Virginia charging ROBB with one count of Wire Fraud in violation of 18 U.S.C. § 1343, along with an arrest warrant. *See* Case No. 1:24-MJ-100. On March 20, 2024, I and other FBI Special Agents located and arrested ROBB at the ARIA Resort and Casino in Las Vegas, Nevada, pursuant to the arrest warrant issued with the complaint.

7. Prior to the arrest, I conferred with security personnel at the ARIA and provided them with ROBB's identifying information. They confirmed that ROBB had a reservation and reported that while he had not yet checked in, he had left luggage with the ARIA Resort and Casino's bellhop service.

8. FBI special agents observed ROBB at the ARIA and approached him at approximately 2:15 PM PT. During a search incident to arrest, agents located an Apple iPhone cellular telephone and wallet on ROBB's person.

9. Employees for the ARIA Resort and Casino informed the FBI that after ROBB's arrest, they considered his luggage to be abandoned property. They then turned over ROBB's luggage to myself and other special agents.

10. The luggage included two black suitcases, a toiletry bag, and a black laptop bag, which ROBB had provided to the ARIA Resort and Casino bellhop service. At least one of the suitcases was labeled with a tag containing ROBB's name and address. ROBB was transported for processing without incident. ROBB's luggage was transported to the FBI Las Vegas Field Office where it was secured according to FBI protocols and where it is presently located.

11. On March 21, 2024, the Honorable Daniel Albregts, United States Magistrate Judge for the District of Nevada authorized a search warrant for the black laptop bag associated with ROBB. The warrant authorized the search of the laptop bag and seizure of any electronic devices and storage media contained in the black laptop bag that are evidence of violations of the Specified Federal Offenses. Members of the FBI executed the search of the laptop bag on March 22, 2024; inside the laptop bag were the **SUBJECT DEVICES**, as well as other devices.

B. Search Warrant Issued on April 1, 2024

12. On April 1, 2024, the Honorable Ivan D. Davis, United States Magistrate Judge for the Eastern District of Virginia authorized a search warrant for the devices seized from the black laptop bag associated with the ROBB, including the **SUBJECT DEVICES**. However, that warrant incorrectly identified the **Apple iPad** as having the serial number GG7FK29GQ16K (instead of GG7FK29GQ16X, where the last letter is an X and not a K) and the Predator Helios Neo 16 laptop as having the serial number NGQMAAA0013140C5E77600 (instead of NHQMAAA0013140C5E77600, where the second letter is H instead of G). Upon reviewing the **SUBJECT DEVICES** in preparation to search them, law enforcement realized the error.[1] Law enforcement now seeks this search warrant for a search of the devices with the correct serial

[1] The Predator Helios Neo 16 laptop with serial number NHQMAAA0013140C5E77600 has been imaged by FBI personnel in preparation for review but has yet to be searched.

numbers listed in an abundance of caution. The probable cause detailed in this warrant does not differ from the probable cause laid out in the April 1 warrant, though the discussion of the devices has been updated accordingly.

C. Case Background & Summary

13. In or around January 2003, ROBB pleaded guilty to two counts of wire fraud in the United States District Court for the Northern District of California. ROBB was sentenced to 27 months and ordered to pay $4.1 million in restitution to 18 victims. According to publicly available records, ROBB defrauded investors by falsely stating Las Vegas based casinos would be using his prototype gambling machine and that he had received endorsements from well-known figures. Contrary to his representations to his investors, ROBB used investor funds to gamble in Las Vegas and to buy new vehicles. When investors refused to invest more money, ROBB threatened investors' lives and safety.

14. In or around December 2023, FBI was alerted to a criminal scheme through which ROBB solicited investment in a Maximum Extractable Value (MEV) cryptocurrency trading bot (hereafter the "MEV bot"). In my training and experience, I know MEV cryptocurrency trading bots are software tools that analyze arbitrage opportunities by manipulating the sequence of transactions within a blockchain block and subsequently execute strategic transactions to produce a profit. The FBI's ongoing investigation included, in part, interviews with victims and witnesses, a review of documents and communications provided by victims and witnesses, and analysis of bank and virtual currency exchange account records.

15. The ways, manner, and means by which ROBB sought to accomplish the scheme and its objectives included, but were not limited to, the following:

a. ROBB recruited prospective investors by touting his own experience and expertise, his purported success in various cryptocurrency and Web3 projects he managed or contributed to, and his purported association with well-known and reputable individuals within the cryptocurrency investment space.

b. ROBB made materially false, fraudulent, and misleading representations—and material omissions—about the progress and capabilities of the MEV bot, the timing of when he planned to "launch" the bot, how investors' money would be used, and the profits investors would supposedly realize through the MEV bot.

c. ROBB obfuscated the location and use of investment funds through the use of multiple virtual currency addresses, virtual currency exchange accounts, and bank accounts.

d. ROBB concealed and misrepresented the true disposition of investor funds. Specifically, ROBB used investor funds to pay for personal expenses such as luxury vacations, vehicles, and a luxury suite at the Denver Broncos football stadium.

D. Investor Complaints

16. The FBI has received numerous investor complaints from more than ten investors alleging losses totaling more than $2.2 million. These complaints include allegations of misrepresentations and misuse of investor funds for personal expenses. Through its own review of financial records and interviews with investors, the FBI has identified about $1.5 million in funds it has either confirmed or believes were from investors, though investigation is still ongoing. Some of the investor complaints are summarized as follows:

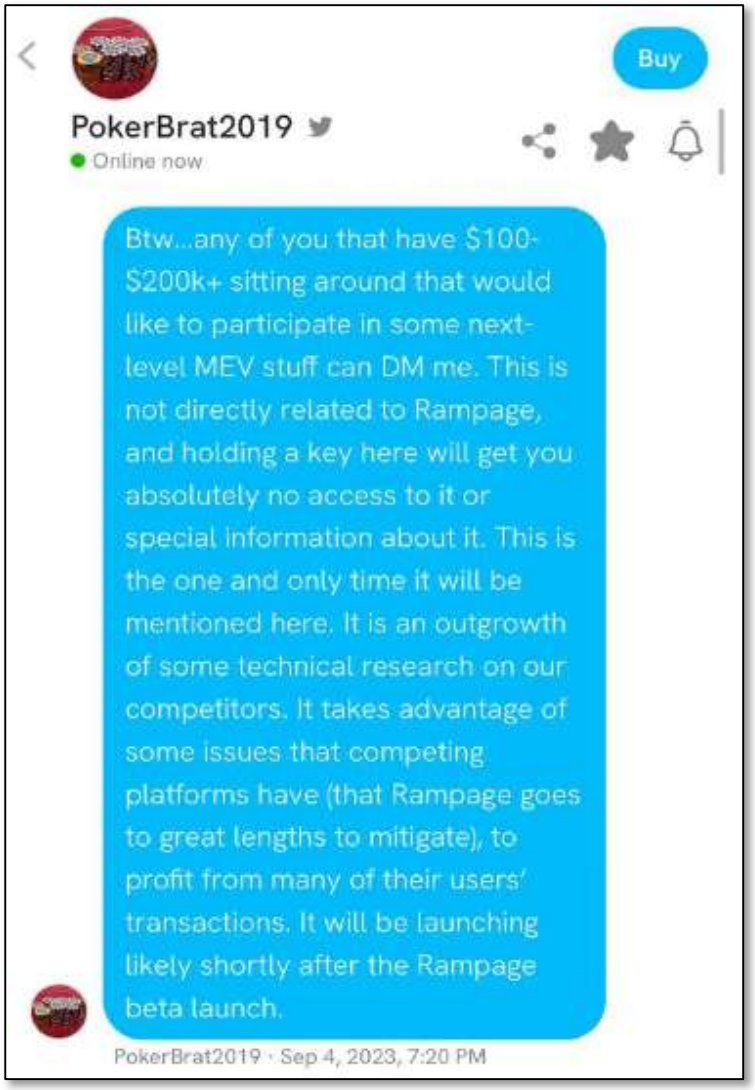
Investor A

17. Investor A is a resident of Brambleton, Virginia, which is within the Eastern District of Virginia. At all times that Investor A was communicating with ROBB other than September 7-10, 2023, Investor A was located within the Eastern District of Virginia. In or around September

2023, Investor A purchased keys to ROBB's Friend.Tech account "PokerBrat2019." In my training and experience, I know Friend.Tech is a blockchain-based social platform. Its main feature is "token-gated chats" through tokens called "keys" that can be purchased and traded. Users gain access to other users' token-gated chats through the purchase of keys. In other words, Friend.Tech allows users to purchase access to chat rooms with specific individuals.[2]

18. On or around September 4, 2023, ROBB posted in his Friend.Tech chat advertising an opportunity to invest in a Maximum Extractable Value (MEV) cryptocurrency trading bot. ROBB invited individuals that have "$100-$200k+ sitting around" and would like to "participate in some next-level MEV stuff" to send him a direct message to learn more. A screenshot containing ROBB's representations on Friend.Tech is included below:

[2] ROBB has received income from the sale of access to his Friend.Tech account. As of February 2024, it appears he has received approximately $150,000. This information is publicly available through Friend.Tech. Law enforcement has not identified this money being transferred into ROBB's bank accounts.

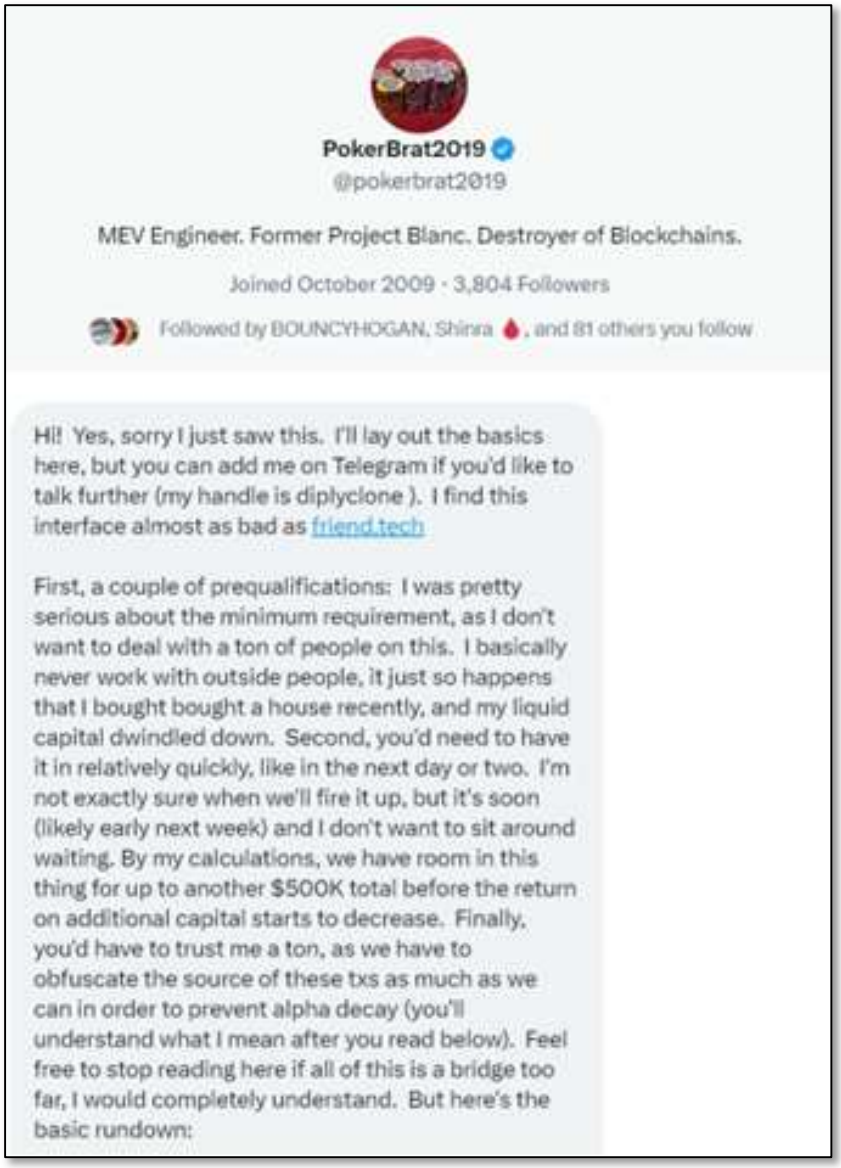


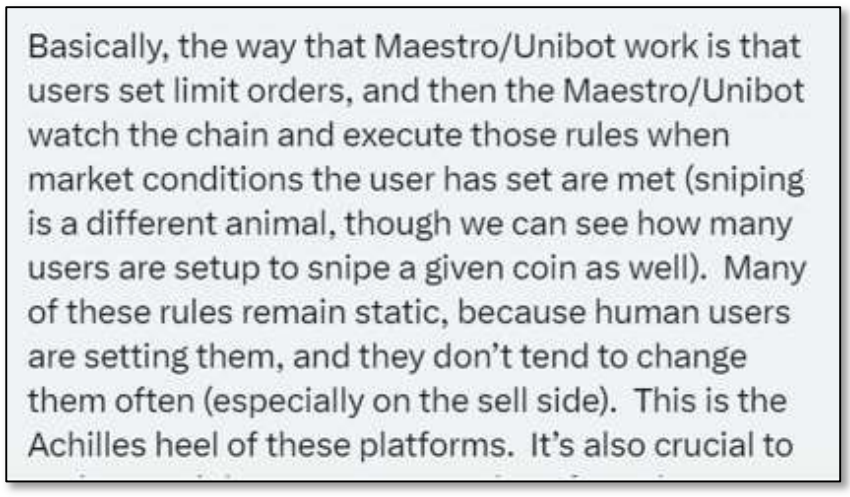
19. A review shows that on September 4, 2023, the same day ROBB sent the above message, ROBB accessed his Coinbase account from an IP address geolocated in Las Vegas, Nevada.

20. In ROBB's Friend.Tech message, as shown above, ROBB references an entity called "Rampage." Based on information obtained in this investigation, I know that Rampage is a separate automated cryptocurrency trading platform that ROBB advertised but also failed to launch.

21. On or about September 7, 2023, Investor A sent a direct message to ROBB's X account, @pokerbrat2019, and discussed the opportunity to invest in the MEV bot. While communicating on X, ROBB made multiple representations to Investor A about the MEV bot and told Investor A that the investment must total at least $100,000.

22. ROBB explained to Investor A how the MEV bot would work, how Investor A's investment would be used by as capital by the MEV bot to trade cryptocurrency, how the origin of Investor A's investment must be "obfuscate[d]," and how ROBB and Investor A would split profits. Further, ROBB told Investor A that the MEV bot would make millions of dollars and assured Investor A that this was a low-risk investment. Additionally, ROBB insisted Investor A must invest within a "day or two," because he expected the bot to be operational "soon (likely early next week)." In my training and experience, I know that individuals engaged in investment fraud will often seek to create a sense of urgency with investors so that investors are pressured to invest quickly without asking questions that may alert the investor to the truth about the investment. Screenshots containing ROBB's representations on X to Investor A are included below:


PokerBrat2019
@pokerbrat2019
MEV Engineer. Former Project Blanc. Destroyer of Blockchains.
Joined October 2009 · 3,804 Followers
Followed by BOUNCYHOGAN, Shinra , and 81 others you follow
Hi! Yes, sorry I just saw this. I'll lay out the basics here, but you can add me on Telegram if you'd like to talk further (my handle is diplyclone). I find this interface almost as bad as friend.tech
First, a couple of prequalifications: I was pretty serious about the minimum requirement, as I don't want to deal with a ton of people on this. I basically never work with outside people, it just so happens that I bought bought a house recently, and my liquid capital dwindled down. Second, you'd need to have it in relatively quickly, like in the next day or two. I'm not exactly sure when we'll fire it up, but it's soon (likely early next week) and I don't want to sit around waiting. By my calculations, we have room in this thing for up to another $500K total before the return on additional capital starts to decrease. Finally, you'd have to trust me a ton, as we have to obfuscate the source of these txs as much as we can in order to prevent alpha decay (you'll understand what I mean after you read below). Feel free to stop reading here if all of this is a bridge too far, I would completely understand. But here's the basic rundown:


Basically, the way that Maestro/Unibot work is that users set limit orders, and then the Maestro/Unibot watch the chain and execute those rules when market conditions the user has set are met (sniping is a different animal, though we can see how many users are setup to snipe a given coin as well). Many of these rules remain static, because human users are setting them, and they don't tend to change them often (especially on the sell side). This is the Achilles heel of these platforms. It's also crucial to

understand that most transactions from these platforms are private - they bypass the public mempool. This ostensibly sidelines MEV bots - after all, if we can't see the transactions, we cannot profit from them. But if we were the only ones to see them, we would have no competition and would make millions.

So I wrote something to figure out which addresses are using these services, and then it watches their trades on-chain to extrapolate the rules that each user has set. I can backtest how accurate these predictions are, without risking a single dime. I have been doing exactly this over the past few weeks, and I'm up to ~93% accuracy (when it makes a prediction). It's theoretically good enough already to make enormous returns, but I am pushing to get it to ~95%. I expect to hit that within a day or two of the Rampage launch. Since we can predict what they are going to buy or sell, when, the gas price at which they will do it, and in what amounts, even though we cannot see their transactions, we can still profit from them. We can backrun them, hijack any backruns the platform itself was going to do, sandwich them, etc. We will be the only people doing it, because nobody else knows the transaction exists. Backrunning is normally enormously competitive, but we'll have zero competition. Backrunning just means landing a transaction behind their buy that does an arbitrage with a different pair that has a lower price than the pair they bought from.

Additionally, there is a tremendous amount of overlap in these orders. We can warehouse tokens their users are actively buying, because we know what will trigger them to buy or sell. When they buy, we can dump on them. There are a few bots making up to 6 figures per day doing this, but they are doing it with fierce competition. We have none for this because nobody can see the txs we are targeting. I call this a "blind delayed sandwich". We know which tokens are most active among their users, and what conditions will make them buy or sell. We can hold the correct tokens and always make a profit when those transactions inevitably occur, and we can even cause those transactions to occur by pushing prices around because we know how much of what tokens will be bought or sold when the price hits a certain number.

So, this is all well and good but quite capital intensive. It also involves some holding risk, although it's very close to zero because the activity gets so concentrated through these bots (everyone is going after the same thing).

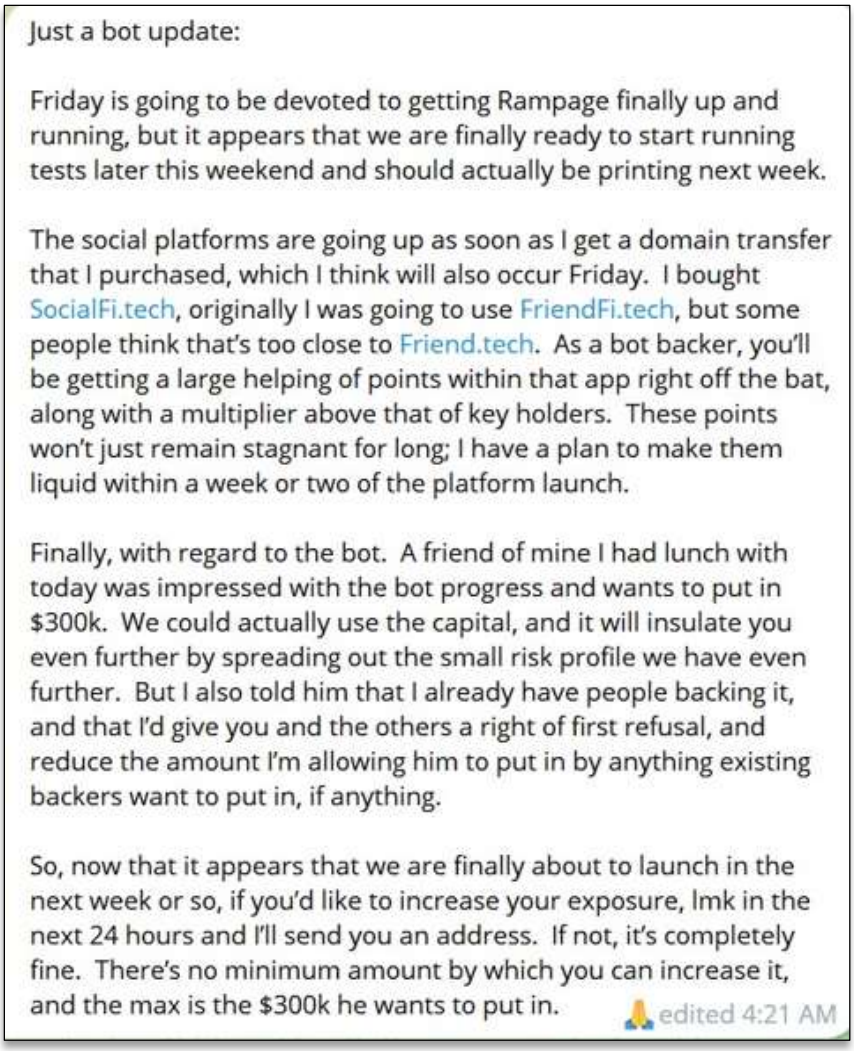
Lmk if you'd like to move forward. Basically you'd get 50% of the profits attributable to your portion of the bankroll, which is currently around $800K.

23. Investor A and ROBB continued their communication on Telegram. ROBB used the Telegram name "DiplyClone." On Telegram, ROBB provided Investor A an Ethereum virtual currency address to send his initial $100,000 investment. On or about September 8, 2023, Investor A sent ROBB an amount of USD Coin (USDC) totaling approximately $100,000. The funds

provided by Investor A were subsequently transferred through multiple virtual currency addresses and then into ROBB's Coinbase account.

24. In the weeks that followed, ROBB repeatedly promised Investor A that the MEV bot would be launched shortly, and then subsequently provided multiple excuses for why the MEV bot had not yet launched. Among other things, ROBB claimed he was dealing with an illness and facing other issues in the Rampage development process that required his attention. In my training and experience, I know that individuals engaged in investment fraud will often seek to conceal the true status of the investment, such as the progress and launch of the bot, so that they can continue the fraud and avoid alerting investors to the true disposition of the funds.

25. On or around October 27, 2023, ROBB told Investor A that a new investor was interested in making a $300,000 investment in the MEV bot. Such an investment would dilute Investor A's profits, so ROBB gave Investor A the chance to make an additional investment. ROBB also told Investor A the MEV bot would launch "in the next week or so." On or around October 28, 2023, Investor A sent an additional $50,000 to an Ethereum virtual currency address provided by ROBB. The funds provided by Investor A were subsequently transferred through multiple virtual currency addresses and then into ROBB's Coinbase account. A screenshot containing ROBB's October 27 representations on Telegram are included below:



Just a bot update:

Friday is going to be devoted to getting Rampage finally up and running, but it appears that we are finally ready to start running tests later this weekend and should actually be printing next week.

The social platforms are going up as soon as I get a domain transfer that I purchased, which I think will also occur Friday. I bought SocialFi.tech, originally I was going to use FriendFi.tech, but some people think that's too close to Friend.tech. As a bot backer, you'll be getting a large helping of points within that app right off the bat, along with a multiplier above that of key holders. These points won't just remain stagnant for long; I have a plan to make them liquid within a week or two of the platform launch.

Finally, with regard to the bot. A friend of mine I had lunch with today was impressed with the bot progress and wants to put in $300k. We could actually use the capital, and it will insulate you even further by spreading out the small risk profile we have even further. But I also told him that I already have people backing it, and that I'd give you and the others a right of first refusal, and reduce the amount I'm allowing him to put in by anything existing backers want to put in, if anything.

So, now that it appears that we are finally about to launch in the next week or so, if you'd like to increase your exposure, lmk in the next 24 hours and I'll send you an address. If not, it's completely fine. There's no minimum amount by which you can increase it, and the max is the $300k he wants to put in. 🙏 edited 4:21 AM

26. On or around November 7, 2023, ROBB informed Investor A that he was going to start testing the bot that evening. Investor A responded that he was looking forward to seeing the evidence of the transactions. Early the next morning, ROBB informed Investor A that the bot had not yet conducted any transactions because it was still "warming up."

27. On or around November 8, 2023, Investor A requested a refund from ROBB because they had not received any returns or evidence ROBB created a MEV bot. ROBB provided multiple excuses for why he could not immediately refund Investor A; for example, ROBB claimed to be a victim of extortion attempts and insisted his virtual currency exchange account was frozen.

Despite ROBB repeatedly promising him his refund by various dates, as of the date of this affidavit, Investor A has not received a refund from ROBB nor profits from the MEV bot.

Investor B

28. In October 2022, Investor B received a message from ROBB's X account, @pokerbrat2019, seeking investment in a MEV bot. Similar to the statements made to Investor A, ROBB told Investor B he created a MEV cryptocurrency trading bot that would generate millions of dollars in profit. ROBB told Investor B their investment would be used by the MEV bot to execute trades and move the market. Profits from the MEV bot would be split "fifty-fifty" between ROBB and Investor B. ROBB made representations to Investor B that are similar in nature to those captured in the screenshots provide by Investor A.

29. From in and around November 2022 to June 2023, Investor B invested a total of approximately $514,443 with ROBB. From November 2022 to May 2023, Investor B sent multiple USDC transactions totaling approximately $411,943 to Ethereum addresses provided by ROBB. A review of records shows ROBB transferred the funds through multiple virtual currency addresses before depositing the funds at ROBB's Binance account. From April 2023 to June 2023, Investor B sent approximately eight wires totaling $132,500 to ROBB's personal bank accounts. For example, on April 13, 2023, Investor B wired $50,000 from his Bank of America account to ROBB. This wire transfer was routed through a server located in the Eastern District of Virginia.

30. Investor B and ROBB met in person on two occasions. During their interactions, ROBB assured Investor B the MEV bot would be launched imminently. When the MEV bot failed to launch within months, ROBB provided Investor B multiple excuses for why the MEV bot was not developed or launched, including an alleged suicide attempt by ROBB's sister.

31. In and around September 2023, approximately 10 months after Investor B's initial investment, Investor B approached ROBB about a refund. Investor B had not received any money

from ROBB nor any indication the MEV bot was developed. On September 27 and October 13, 2023, Investor B received a partial refund from ROBB totaling $75,000. As of the date of this affidavit, Investor B had not received the remaining $439,443 owed by ROBB nor any profits from the MEV bot.

Investor C

32. In and around September 2023, Investor C saw a post by ROBB on Friend.Tech advertising an opportunity to invest in a MEV bot. Through conversations on Friend.Tech, X, and Telegram, ROBB told Investor C, among other representations, that Investor C's investment would be used by the MEV bot to execute trades. ROBB claimed the bot was almost ready to go and the trades would result in "six figure returns" within a week. Further, ROBB described Investor C's investment in the MEV bot as a "risk free" investment. ROBB's representations to Investor C are similar in nature to those captured in the screenshots provided by Investor A.

33. ROBB told Investor C their investment must be sent to an Ethereum virtual currency address operated by ROBB and then through other virtual currency addresses. As with Investor A, ROBB claimed he must "obfuscate" the funds or else the MEV bot strategy would be "ruined." On or about September 5, 2023, Investor C sent approximately $100,000 to ROBB for investment in the MEV bot.

34. Approximately two months later, ROBB informed Investor C that new investors were investing significant funds that would dilute Investor C's initial investment and that Investor C needed to invest more money. Investor C therefore invested an additional $25,000 in the MEV bot on or about November 2, 2023. At this time, ROBB assured Investor C that the release of the bot was a matter of when, not if. At this moment, Investor C was worried ROBB would run away with their money.

35. A review of records shows that upon receipt of funds from Investor C, ROBB sent the funds through multiple virtual currency addresses before depositing the funds to ROBB's Coinbase account.

36. Investor C tried to get a refund from ROBB, but ROBB refused. In January 2024, ROBB requested Investor C invest more money in the MEV bot, but Investor C declined. As of February 26, 2024, Investor C had not received any funds from ROBB nor profits from the MEV bot. Investor C has stated that if he knew at the time he made his investments that ROBB still would not have launched the bot by now, he would not have invested.

37. The FBI has interviewed and/or received complaints from approximately eight other individuals who similarly reported being induced by ROBB to invest in an MEV bot. These individuals have not received profits from the investment or refunds when requested.

E. Laundering of Funds Derived from the Fraud, Including Use of Investor Funds for Personal Expenses

38. A review of account records and statements for numerous bank and virtual currency exchange accounts associated with ROBB shows ROBB received approximately $1.5 million from individuals I have confirmed or believe to be investors in ROBB's MEV bot, based on interviews of investors, correspondence received from third parties, and similarities among the transactions. Despite ROBB's representations to investors claiming investor funds would be used as trading capital for the MEV bot, the records show that investor funds were funneled to virtual currency exchange accounts and traditional bank accounts held in ROBB's name. The funds were ultimately used to pay for personal expenses. There is no evidence that any of these funds were ever used for trading.

39. Through conversations with investors, records provided by virtual currency exchanges and banks, and analysis of records and the blockchain, I learned ROBB used multiple

virtual currency addresses, virtual currency exchange accounts and bank accounts as well as the purchase of goods to launder proceeds of the criminal scheme. Specifically, ROBB transferred investor funds between multiple virtual currency addresses, deposited funds to his virtual currency exchange accounts, split funds between different accounts, and then ultimately transferred the investor funds to his personal bank accounts. Because the blockchain is otherwise public, these numerous transfers and mixing of funds made it difficult for any of his investors to track their funds and realize they were not being used for the promised purposes. From his personal bank accounts, ROBB used investor funds to make personal purchases as described in Section III. In my training and experience, I know that individuals use electronic devises to move funds, via interstate wires, between multiple accounts to obscure the source of funds and disguise ownership in an attempt to launder illicit proceeds. As noted above, ROBB told some investors that he needed to "obfuscate" the source of funding.

40. For example, on or about September 8, 2023, at ROBB's direction, Investor A sent three transactions of USDC totaling approximately $100,000 to an Ethereum virtual currency address ending in -f147 ("Ethereum Address 1"). In three transactions executed between September 26 and October 3, 2023, ROBB transferred the funds to three separate Ethereum addresses; from there, ROBB transferred the funds to his Coinbase account. The transfers are summarized as follows:

a. On September 26, 2023, ROBB transferred 50,000 USDC from Ethereum Address 1 to an Ethereum virtual currency address ending in -e183. Within minutes, the funds were deposited into ROBB's Coinbase account. That same day, ROBB transferred $20,000 from his Coinbase account to his Bank of America bank account, $5,000 to his Wells Fargo bank account, and $5,000 to his JPMorgan Chase bank account.

b. On September 27, 2023, ROBB transferred 25,000 USDC from Ethereum Address 1 to an Ethereum address ending in -690F. Within minutes, the funds were deposited into ROBB's Coinbase account.

c. On October 3, 2023, ROBB transferred 25,004 USDC from Ethereum Address 1 to an Ethereum virtual currency address ending in -4712. Within minutes, the funds were deposited into ROBB's Coinbase account.

41. On October 28, 2023, at ROBB's direction, Investor A sent a 50,000 USDC transaction totaling approximately $50,000 to an Ethereum virtual currency address ending in -dcDe ("Ethereum Address 2"). Through five transactions executed within the next 11 days, ROBB transferred the USDC in Ethereum Address 2 to two Ethereum virtual currency addresses, from which ROBB transferred the funds to his Coinbase account. The transfers are summarized as follows:

a. From October 29 to November 3, 2023, ROBB transferred 35,000 USDC from Ethereum Address 2 to an Ethereum address ending in -80DF.

b. From November 6 to 8, 2023, ROBB transferred 15,000 USDC from Ethereum Address 2 to an Ethereum address ending in -717E.

c. Within minutes of receipt, the two Ethereum addresses sent the funds received from Investor A to ROBB's Coinbase account.

42. A review of ROBB's Coinbase account reveals that ROBB transferred funds received Investor A to ROBB's bank accounts at Wells Fargo, JPMorgan, and Bank of America. A review of financial statement from ROBB's bank accounts shows ROBB used funds from Investor A for purposes not disclosed to or approved by Investor A, to include airline tickets, sporting event tickets, and purchases at casinos.

43. From November 2022 through January 2024, ROBB deposited approximately $1.1 million in this manner into his personal Bank of America bank account and approximately $417,900 into a personal JPMorgan Chase bank account.

44. Further, a review shows ROBB spent large sums of investor money on personal expenses. Some examples of ROBB using investor funds for personal expenses are summarized as follows:

a. Between September 4 and 5, 2023, ROBB received three deposits to his Coinbase account totaling over $250,000. The funds derived from a payment from an investor known to the FBI and other payments FBI believes are associated with other investors. On September 5, 2023, ROBB executed six transfers totaling $215,924.61 from his Coinbase account to his Bank of America account, which had a prior balance of $6,532.09. On the same day, ROBB sent a wire totaling $204,423 to Stadium Management Company, a management company for Mile High Stadium and the Denver Broncos Football Club. A review of records provided by the Denver Broncos Football Club shows ROBB purchased a two-year lease for an executive suite at the Denver Broncos' Mile High Stadium for the 2023 and 2024 National Football League seasons. ROBB's payment to the Bronco's on September 5 was transmitted through a server located in the Eastern District of Virginia.

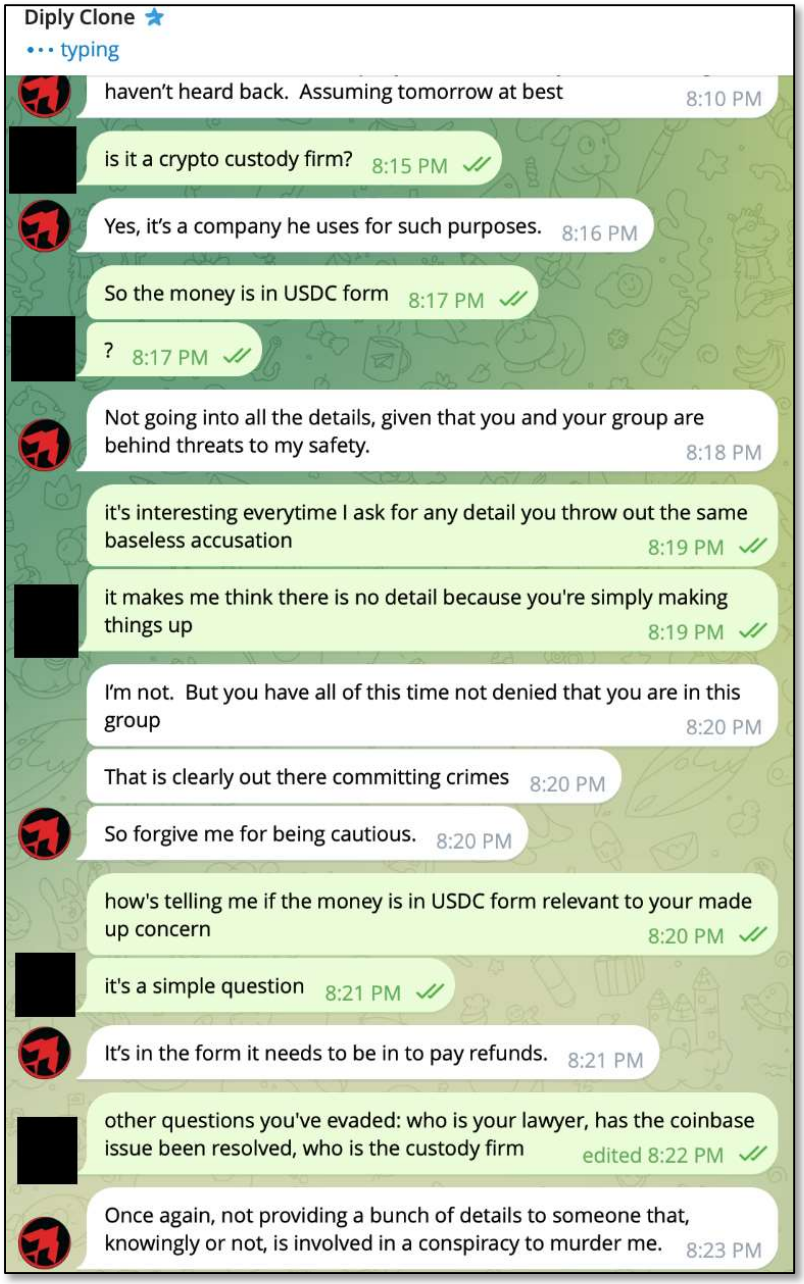
b. On or about September 6, 2023, ROBB received three deposits to his Coinbase account totaling approximately $129,235 that were consistent with investor payments. On the same day, ROBB transferred approximately $126,399.26 from his Coinbase account to JPMorgan Chase account, which had a prior balance of $744.67. On the same day, ROBB made a payment of $117,570.00 from his JPMorgan Chase account

to Stew Hansen Dodge City. A review of records from Stew Hansen Dodge City shows ROBB used the funds to purchase a 2023 Jeep Wagoneer vehicle.

c. From approximately October 8 to October 11, 2023, ROBB received four deposits to his Coinbase account totaling approximately $151,400 that were consistent with investor payments to ROBB. Between October 11 and 12, 2023, ROBB transferred approximately $68,582.52 from his Coinbase account to his Bank of America account. Shortly after, on October 12, 2023, ROBB wired $46,914.50 from his Bank of America account to Atlantis Paradise Vacation. Open-source research shows Atlantis Paradise is an ocean-themed vacation resort on Paradise Island in the Bahamas.

45. Through conversations with victims and witnesses as well as a review of bank and virtual currency exchange account records, I learned ROBB continues to actively provide excuses for MEV bot launch and refund delays. I also learned ROBB is actively soliciting investment from new investors.

46. ROBB actively provides excuses for MEV bot and refund delays to include extortion and threats to his safety. For example, ROBB accused an investor of being involved in a conspiracy to murder ROBB and accused another investor of reporting him to the FBI and thus creating legal delays. A screenshot of the Telegram message from ROBB is included below (with the investor's profile picture redacted):



47. In addition to soliciting investment in the MEV bot, ROBB is actively promoting and seeking investment in a new cryptocurrency token "$RAT." ROBB continues to claim large returns for investment in the MEV bot and tokens. For example, I learned from an investor that on or around February 27, 2024, ROBB posted a message about the MEV bot and tokens to Telegram. The message contains an image with the text "poof you're a millionaire" and states being a

millionaire could "easily" be the case for many investors. Further, ROBB implied the returns are imminent, stating that "sometime tonight, this journey begins!" A screenshot containing the image and ROBB's Telegram message is included below:

48. A review of ROBB's Coinbase account shows that as of February 2024, ROBB continues to receive large payments of Ether (ETH), USDC, and Solana (SOL). Due to the ongoing solicitation of investment through Telegram, the similarity in volume between known investor payments and the recent payments, and a lack of other identifiable income, I believe ROBB actively receives investment payments from new investors and will continue to solicit investment from additional investors.

FORENSIC ANALYSIS

49. As further described in Attachment B, this application seeks permission to locate not only electronically stored information that might serve as direct evidence of the crimes described on the warrant, but also forensic evidence that establishes how the **SUBJECT DEVICES** were used, the purpose of its use, who used it, and when.

50. *Probable Cause*. Based on my knowledge, training, and experience, as well as information related to me by agents and others involved in this investigation and in the forensic examination of digital devices, I respectfully submit that there is probable cause to believe that the records and information described in Attachment B will be stored in the electronic storage media and digital devices for at least the following reasons:

a. Based upon my knowledge, training, and experience as well as my discussions with others involved in financial crime investigations, I know that subjects involved in financial crime in the manner described above will often store records of encrypted communications platform messages, social media messages, text messages, SMS messages, and emails within electronic devices, including cellular telephones, laptops, computers, and tablets. As discussed above, ROBB himself communicated with his investors almost entirely through written communications on various messaging platforms.

b. ROBB has solicited money from purported investors in cryptocurrency. Tracing of those investments indicated that ROBB would transfer that cryptocurrency through unhosted wallets, i.e., wallets not maintained by a third-party exchange, but instead held within ROBB's own control. Based on my training and experience, I know that such wallets can be stored on electronic devices. Additionally, I know that

individuals who use unhosted wallets will often store the "seed phrases" that allow the person holding the seed phrase to access and control those wallets on their electronic devices.

c. ROBB has represented that he is creating a MEV bot. Such a bot would require a computer to program and operate. Developers will frequently back up any programs that they are developing to other storage media to guard against loss. Developers are also likely to protect their projects using encryption, passwords, or other data security devices. Evidence of such passwords or the data security devices themselves are frequently stored with the electronic devices, as the likely threat is often perceived to be digital (e.g., hacking) rather than physical.

d. Cellular telephones are often programmed for speed dialing, contain contact lists, and recent call activity that persons involved in criminal activity who sell firearms, and those who aid and abet their activities, frequently take, or cause to be taken, photographs and/or videos that provide evidence of their criminal conduct, such as images/videos depicting their association with conspirators; images/videos depicting displays of their illegally obtained wealth; or screenshots of conversations depicting or reflecting the fraudulent scheme.

e. Individuals who engage in the foregoing criminal activity, in the event that they change computers, will often "back up" or transfer files from their old computers' hard drives to that of their new computers or to other external storage media, so as not to lose data, including that described in the foregoing paragraph, which would be valuable in facilitating their criminal activity.

f. Computer, smart phone, and other digital device files, or remnants of such files, can be recovered months or even years after they have been downloaded onto an electronic storage medium, deleted, or viewed via the Internet. Electronic files downloaded to an electronic storage medium can be stored for years at little or no cost. Even when such files have been deleted, they can be recovered months or years later using readily available forensics tools. When a person "deletes" a file on a digital device such as a home computer, the data contained in the file does not actually disappear; rather, that data remains on the electronic storage medium until it is overwritten by new data.

g. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space – that is, in space on the electronic storage medium that is not allocated to an active file or that is unused after a file has been allocated to a set block of storage space – for long periods of time before they are overwritten. In addition, a digital device's operating system may also keep a record of deleted data in a "swap" or "recovery" file. Similarly, files that have been viewed via the Internet are automatically downloaded into a temporary Internet directory or "cache." The browser typically maintains a fixed amount of electronic storage medium space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages. Thus, the ability to retrieve "residue" of an electronic file from an electronic storage medium depends less on when the file was downloaded or viewed than on a particular user's operating system, storage capacity, and computer, smart phone, or other digital device habits.

h. Wholly apart from user-generated files, computer storage media—in particular, computers' internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory "swap" or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

51. *Forensic evidence*. As further described in Attachment B, this application seeks permission to search for not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how the **SUBJECT DEVICES** were used, the purpose of its use, who used it, and when. There is probable cause to believe that this forensic electronic evidence will be on the **SUBJECT DEVICES** because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage

media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the "who, what, why, when, where, and how" of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This "user attribution" evidence is analogous to the search for "indicia of occupancy" while executing a search warrant at a residence.

c. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculpating or exculpating the computer owner.

d. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log: computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows

investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation.

e. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculpate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

f. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

g. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an

accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

h. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

i. I know that when an individual uses a computer to possess or receive child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain: data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

52. *Nature of examination*: Based on the foregoing, and consistent with Rule 41(e)(2)(B), the

warrant I am applying for would permit the examination of the device consistent with the warrant. The examination may require authorities to employ techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of the device to human inspection in order to determine whether it is evidence described by the warrant.

53. *Manner of execution*: Because this warrant seeks only permission to examine a device already in law enforcement's possession, the execution of this warrant does not involve the physical intrusion onto a premise. Consequently, I submit there is good cause for the Court to authorize execution of the warrant at any time in the day or night.

(Continued on next page)

CONCLUSION

Based on the information contained herein, I respectfully submit that there is probable cause to believe that the **SUBJECT DEVICES**, described in Attachment A, contain evidence, fruits, and instrumentalities of violations of the Specified Federal Offenses. Therefore, I respectfully request that the attached warrant be issued authorizing the search and seizure of the items listed in Attachment B.

Because the **SUBJECT DEVICES** are in the FBI's custody and control, good cause exists for the warrant to be executed at any time of the day or night.

Respectfully submitted,

Jordan A Jenkins

Jordan Jenkins
Special Agent
Federal Bureau of Investigation

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by telephone on May 30, 2024.

Hon. William B. Porter
United States Magistrate Judge

ATTACHMENT A

Property to Be Searched

The property to be searched are the **SUBJECT DEVICES**, one Apple iPad Serial # GG7FK29GQ16X and one Predator Helios Neo 16 laptop Serial # NHQMAAA0013140C5E77600, currently located at the Federal Bureau of Investigation, Washington Field Office, Northern Virginia Resident Agency, in Manassas, Virginia.

This warrant authorizes the forensic examination of the **SUBJECT DEVICES** for the purpose of identifying the electronically stored information described in Attachment B.

ATTACHMENT B

List of Items to be Seized and Searched

Items constituting fruits, evidence, or instrumentalities of violations of the Specified Federal Offenses including but not limited to the following:

1. Records and information relating to cryptocurrency, trading bots, and financial activity;

2. All bank records, checks, credit card bills, account information, and other financial records, including records pertaining to cryptocurrency accounts and/or wallets and information such as seed phrases that may be used to reconstitute or access those wallets to examine their contents;

3. All communications concerning the above-described investment scheme, including, but not limited to, references to a cryptocurrency trading bots, investment opportunities, the disposition of investor funds, and the transfer and use of cryptocurrency and funds related to the investment scheme;

4. Records and information relating to the development of a MEV cryptocurrency trading bot, including whether such a bot actually exists;

5. Records and information related to the laundering and disposition of investor funds, including potential assets representing the proceeds of the Specified Federal Offenses or property involved in the Specified Federal Offenses;

6. Internet usage records, usernames, logins, passwords, e-mail addresses, and identities assumed for purposes of communication on the Internet, billing, account, and subscriber records, chat room logs, chat records, membership in online groups, clubs or services, connections to online or remote computer storage, and electronic files;

7. Address books, names, and lists of names and address of individuals who may have been contacted by the computer and internet websites;

8. Records and information relating to membership in online groups, social media platforms, and encrypted communication applications;

9. Records and information relating to any online storage or communication accounts used to communicate about and effectuate the Specified Federal Offenses;

10. Records and information that constitute evidence of the state of mind of ROBB, e.g., intent, absence of mistake, or evidence indicating preparation or planning, or knowledge and experience, related to the criminal activity under investigation;

11. Records and information that constitute evidence concerning persons who either (i) collaborated, conspired, or assisted (knowingly or unknowingly) the commission of the criminal activity under investigation; or (ii) communicated with ROBB about matters relating to the criminal activity under investigation, including records that help reveal their whereabouts; and

12. Evidence of who used, owned, or controlled the SUBJECT DEVICES at the time the item described in this warrant was created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, chat, instant messaging logs, photographs, and correspondence;

13. Evidence of software, or the lack thereof, that would allow others to control the SUBJECT DEVICES, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;

14. Evidence indicating how and when the SUBJECT DEVICES were accessed or used to determine the chronological context of computer access, use, and events relating to crime under investigation and to the computer user;

15. Evidence of the attachment to the SUBJECT DEVICES of other storage devices or similar containers for electronic evidence;

16. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the SUBJECT DEVICES;

17. Evidence of the times the SUBJECT DEVICES were used;

18. Passwords, encryption keys, and other access devices that may be necessary to access the SUBJECT DEVICES or programs on the SUBJECT DEVICES;

19. Records of or information about Internet Protocol addresses used by the SUBJECT DEVICES;

20. Records of or information about the SUBJECT DEVICES' Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses; and

21. Contextual information necessary to understand the evidence described in this attachment.

The authorization includes the seizure and search of electronic data to include deleted data, remnant data and slack space.

As used above, the terms "records" and "information" includes all forms of creation or storage, including any form of computer or electronic storage (such as hard disks or other media that can store data); any handmade form (such as writing); any mechanical form (such as printing

or typing); and any photographic form (such as microfilm, microfiche, prints, slides, negatives, videotapes, motion pictures, or photocopies).

If the government identifies seized materials that are potentially attorney-client privileged or subject to the work product doctrine ("protected materials"), the Prosecution Team will discontinue review until a Filter Team of government attorneys and agents is established. The Filter Team will have no future involvement in the investigation of this matter. The Filter Team will review seized communications and segregate potentially protected materials, i.e. communications that are to/from an attorney, or that otherwise reference or reflect attorney advice. At no time will the Filter Team advise the Prosecution Team of the substance of any of the potentially protected materials. The Filter Team then will provide all communications that are not potentially protected materials to the Prosecution Team and the Prosecution Team may resume its review. If the Filter Team concludes that any of the potentially protected materials are not protected (*e.g.,* the communication includes a third party or the crime-fraud exception applies), the Filter Team must obtain either agreement from defense counsel/counsel for the privilege holder or a court order before providing these potentially protected materials to the Prosecution Team. This investigation is presently covert, and the government believes that the subject of the search is not aware of this warrant.

This warrant authorizes a review of electronically stored information, communications, other records and information disclosed pursuant to this warrant in order to locate evidence, fruits, and instrumentalities described in this warrant. The review of this electronic data may be conducted by any government personnel assisting in the investigation, who may include, in addition to law enforcement officers and agents, attorneys for the government, attorney support staff, and technical experts. Pursuant to this warrant, the FBI may deliver a complete copy of the disclosed electronic data to the custody and control of attorneys for the government and their support staff for their independent review.